## REMARKS

*Claim Amendments*

Applicants respectfully request entry of the foregoing claim amendments, which are discussed further below. No new matter is introduced.

*Rejections under 35 U.S.C. §101*

Claims 1-39 are rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

In this regard, Applicants request entry of the foregoing amendments to independent claims 1 and 20 and submit that the claims as amended are directed to statutory subject matter.

The Office Action states two grounds for the rejection of independent claim 1: first, that the claim is directed to an apparatus for communication between a sender that is software and a receiver that is human; and second, that the apparatus is "functional descriptive material (i.e. computer program)."

With regard to the first grounds for rejecting independent claim 1, Applicants submit that although the users of the apparatus are human beings, the language of claim 1 makes clear that the claimed subject matter is the component modules of the claim, which may make possible delivery of data to human users. The components of claim 1 are a "communication module," a "mapping module," and a "secret sharing module." An example of such components is shown in Fig. 1, in which there is a mapping module 106, a communication module 107, and a secret sharing module 108. As described at page 5, line 22 through page 6, line 18 of the present Application, these components are part of a computer program running on a physical memory 103 on a computer 101.

Although it is true that independent claim 1 states that "the apparatus communicat[es] between parties comprising at least the sender and the receiver in at least two different working data identifier set domains," such an apparatus of independent claim 1 is directed to the physical components running on memory 103 that enable such communication – and not to the sender or the receiver themselves. It is therefore statutory subject matter.

However, Applicants also observe that the foregoing arguments are not necessarily meant to imply that independent claim 1 requires that the sender is software and the receiver is human. No such language is found in independent claim 1, which is silent on the nature of the sender and receiver; although such language is found in dependent claim 16. As previously stated, independent claim 1 is directed to physical components running on memory 103 that enable communications, and is therefore statutory subject matter. Dependent claim 16, although it does specify the nature of the sender and receiver, is also statutory subject matter, because like its parent claim 1 it is directed to physical components for enabling communications between such a sender and the receiver.

The second grounds for rejecting independent claim 1 (and also dependent claim 16) is that the apparatus is "functional descriptive material (i.e. computer program)." Applicants submit that the addition of language to independent claim 1 by the foregoing amendments addresses this rejection. In particular, applicants have added language that each of the modules of claim 1 is "stored on a computer-readable medium." Such language finds support at page 5, line 22 through page 6, line 18 of the present Application, among other places; no new matter is added.

Applicants therefore submit that independent claim 1 as amended and all of its dependent claims are directed to statutory subject matter.

Independent method claim 20 is rejected on similar grounds to claim 1 as being "functional descriptive material (i.e. computer program)." Applicants submit that the addition of language to independent claim 20 by the foregoing amendments addresses this rejection. In particular, applicants have added language that each of the elements of claim 20 involve using a component "stored on a computer-readable medium." Such language finds support at page 5, line 22 through page 6, line 18 of the present Application, among other places; no new matter is added.

Applicants therefore submit that independent claim 20 as amended and all of its dependent claims are directed to statutory subject matter.

It is therefore submitted that the rejections under 35 U.S.C. § 101 are overcome.

*Rejections under 35 U.S.C. § 103*

Claims 1-2, 7-8, 16-19, 20-21, 25-26, and 24-37 are rejected under 35 U.S.C. § 103 due to U.S. Pat. No. 6,081,793 of Challener *et al.* (here, "Challener *et al.*"). Also, dependent claims 3-4, 9-12, 22-23, and 27-30 are rejected over Challener *et al.* in view of Schneier (cited in previous Office Action); dependent claims 13-15, 31-33, and 38 are rejected over Challener *et al.* in view of Ansell *et al.* (cited in previous Office Action); and dependent claim 39 is rejected over Challener *et al.* in view of Coss *et al.* (EP 0 909 074 A1).

Applicants respectfully traverse these rejections and request reconsideration and allowance of all claims.

Independent claims 1 and 20 are rejected as obvious over Challener *et al.* In this regard, it is considered useful to give a brief overview of the subject matter of Challener *et al.* Challener *et al.* relates to a technique for creating secure online voting in an election. As described in Fig. 1A, Fig. 7, Fig. 9D, and at Col. 7, line 38 through Col. 8, line 52, the process works by first having a voter register with an authentication server 225 using a smart card 213 that the voter is issued. The authentication server 225 issues the voter with an electronic ballot 235, which the voter then fills out and files electronically with a journal server 227. As shown in Fig. 9D, the voter sends their vote encrypted with the public key of a results server 229, and with the voter's private key; and also sends a voter ID, with the whole package being encrypted with the public key of an authenticator. The journal server 227 therefore receives an encrypted package including both the voter's completed vote, and their voter ID. It then decrypts the package so that it can record the voter ID; but is not allowed access to the contents of the completed vote. It then forwards the completed vote to the results server 229, which decrypts the completed vote and tallies it with other election results.

The journal server 227 therefore performs the role of: (i) receiving an encrypted package that includes both an encrypted completed ballot and an encrypted voter ID; (ii) stripping the voter ID out of the encrypted package that the journal server 227 receives from the voter; and (iii) forwarding only the encrypted completed ballot to the results server 229.

There are, however, several important differences between independent claims 1 and 20, as amended, and Challener *et al.* Applicants therefore submit that Challener *et al.* does not disclose or suggest the inventions of these claims.

First, Applicants have amended independent claim 1 to include the language "...wherein the communication module is capable of transmitting both the anonymously mapped identifier portion and the unmapped research data portion of the working data to the receiver..." Similar language is included in independent method claim 20.

No such communication module is disclosed or suggested by Challener *et al.*, because Challener *et al.* does not involve transmitting both an anonymously mapped identifier portion and a working data portion of research data to the results server 229. Instead, journal server 227 receives both a completed ballot and a voter ID; and sends only the completed ballot on to a results server 229. Challener *et al.* does not disclose or suggest that the journal server 227 would map the voter ID using an anonymous mapping and send it on to the results server 229 along with the completed ballot. Therefore, Challener *et al.* does not disclose or suggest a communication module capable of transmitting both an anonymously mapped identifier and an unmapped research data portion to a receiver.

This difference of independent claims 1 and 20 provides an important advantage for an embodiment according to the invention. In particular, a user of the invention, such as a medical researcher, can analyze patterns in working data while also being able to determine whether the people whose medical data is being analyzed are the same people from record to record. Thus, for example, a medical researcher using a system of the invention could determine whether high blood pressure (in the working data) was correlated with being overweight (in the working data); and later return to look at other working data for the same individuals who were overweight and had high blood pressure. The latter could only be done if the individuals' medical records received by the receiver contained some kind of identifier portion, even if it is anonymously mapped. Thus, for example, a researcher could return to analyze the record whose identifier portion has been anonymously mapped to "X546919," even if the identifier portion has been rendered anonymous.

By contrast, Challener *et al.*'s results server 229 receives only the completed votes; and does not receive an anonymously mapped identifier with each completed vote. Challener *et al.* therefore does not disclose or suggest a system that would allow such an individualized, yet also anonymous, analysis of data as is possible in an embodiment according to the invention. In Challener *et al.*, the results server 229 simply aggregates all of the completed votes it receives;

and does not allow subsequent analysis, for example, of whether the same person who voted for candidate X also voted "Yes" on a ballot question. Challener *et al.* therefore does not disclose or suggest the inventions of independent claims 1 and 20, because it does not disclose or suggest a communication module that is capable of transmitting both an anonymously mapped identifier portion and an unmapped research data portion of working data to a receiver.

Along these lines, Applicants have added new dependent claims 40 and 41, which point out a related benefit of the foregoing distinction over Challener *et al.*: an embodiment according to the present invention allows the analysis of working data that is formed of plural records, where the individual person to which the records relate is the same person across each record of the plural records. This contrasts with Challener *et al.*, in which one person must be associated with one completed ballot, under the "one person, one vote" principle by which elections operate. Applicants therefore request consideration and allowance of these dependent claims.

Another important difference between the independent claims and Challener *et al.* is that Challener *et al.* does not disclose or suggest the use of secret sharing to control keyholder access to a mapping module. There is no disclosure or suggestion of any secret sharing techniques in Challener *et al.*, which relates entirely to the use of conventional public/private key encryption techniques. In the pertinent art, secret sharing is not the same as conventional public/private key encryption. Applicants respectfully traverse the statement in the Office Action that secret sharing is disclosed in items 379, 391, and 439 of Fig. 7 of Challener *et al.* Instead, item 379 relates to a voter's request for a ballot, which uses a public key; item 391 relates to the authentication server 225 sending an encrypted ballot to the voter, again using conventional public keys; and item 439 relates to a results server 229 tabulating the results of an election. Challener *et al.* therefore does not disclose or suggest the use of secret sharing to control keyholder access to a mapping module, which is recited in both independent claims 1 and 20.

Another difference between the independent claims and Challener *et al.* is found in the addition of language by the current amendments that the mapping module is "capable of accessing both the identifier portion and the research data portion of the working data." Whereas the mapping module of claims 1 and 20 is capable of accessing both portions of the working data, the journal server 227 of Challener *et al.* cannot access the completed ballot, because it can only be decrypted by the results server. Challener *et al.*'s journal server 227 therefore does not

function to have a mapping module anonymously map only one portion of working data, out of at least two working data portions that are fully accessible to the mapping module. It therefore does not disclose or suggest the invention of independent claims 1 and 20 as amended.

Applicants also traverse several statements found in the Office Action. Applicants submit that Col. 7, lines 1-37 of Challener *et al.* does not disclose a mapping module for anonymous mapping as claimed by Applicants, but instead relates to the non-automated technique for ballot voting of Fig. 6 of Challener *et al.*, under which a voter uses a card reader, punches a ballot, etc. Applicants also submit that Col. 7, lines 50-67 does not disclose anonymous mapping as claimed by Applicants, instead relating to a voter issuing an electronic request for a ballot, which does not involve an anonymous mapping.

Finally, Applicants respectfully traverse the definition of "working data identifier set domain" given in the Office Action, and submit that the definition of this claim term should be interpreted by standard claim interpretation techniques rather than being necessarily interpreted according to the language given in the Office Action. Applicants note that the concept of the working data identifier set domain is discussed in the present Application at page 12, line 25 through page 13, line 3, among other places.

For the foregoing reasons, Applicants therefore submit that Challener et al. does not disclose or suggest the inventions of independent claims 1 and 20, and request reconsideration and allowance of those claims. Because dependent claims 2, 7-8, 16-19, 21, 25-26, and 24-37 incorporate the features of claims 1 and 20, they are also allowable for the foregoing reasons.

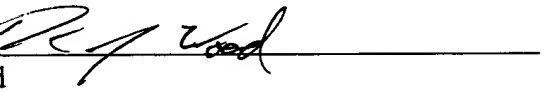
Also, neither Schneier, nor Ansell et al., nor Coss et al., which are applied to several of the dependent claims, discloses or suggests the foregoing features. In particular, those references do not disclose or suggest (i) a communication module capable of transmitting both an anonymously mapped identifier and an unmapped research data portion to a receiver; nor (ii) the use of secret sharing to control keyholder access to Applicants' claimed mapping module; nor (iii) a mapping module such as that claimed by Applicants that is capable of accessing both the identifier portion and the research data portion of the working data; nor the preceding three features in combination. Applicants therefore submit that dependent claims 3-4, 9-15, 22-23, 27-33, 38, and 39 are also allowable for the foregoing reasons.

## CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 
Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 12/7/05